UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/775,172	02/01/2001	See-Wai Yip	3209.2.2	7281

21552 7590 04/28/2005

MADSON & METCALF
GATEWAY TOWER WEST
SUITE 900
15 WEST SOUTH TEMPLE
SALT LAKE CITY, UT 84101

EXAMINER	
NALVEN, ANDREW L	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 04/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/775,172	YIP ET AL.	
	Examiner	Art Unit	
	Andrew L. Nalven	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 November 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-60* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-60* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01 February 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

HL

KH

DETAILED ACTION

1. Claims 1-60 are pending.

Response to Arguments

2. Applicant's arguments with respect to claims 1-60 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-7, 10-26, 29-47, and 50-60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Asay et al US Patent No. 5,903,882 in view of RSA Security's BSAFE Cert-C software as seen in press release "RSA Security Simplifies PKI Application Development" and Lapstun et al US Patent No. 6,549,935.

5. With regards to claims 1, 10, and 41, Asay teaches the integrating of an server with a server-specific certificate authority for issuing server-specific certificates (Asay,

column 10 lines 23-50 "reliance server"), receiving notice of a master certification authority issuing a master certificate to a subscriber (Asay, column 12 lines 17-21), issuing to the subscriber a server-specific certificate for use by the server (Asay, column 10 lines 45-50), and the existence of several servers with integrated certificate authorities (Asay, column 12 lines 23-28). Asay fails to teach the integrating of the certificate authority into an application and the issuing of application-specific certificates. RSA Security teaches the integrating of the certificate authority into an application (RSA Security Press Release, Page 2, Paragraphs 3-4). Lapstun teaches the issuing of application-specific certificates (Lapstun, column 33 lines 53-56, certificate for each application). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize RSA Security's method of integrating PKI functions into an application and Lapstun's certificate method with Asay's reliance server for integrating transactions because it offers the advantage of simplifying and accelerating the development of PKI enabled applications and providing interoperability with all of the leading PKI platforms (RSA Security Press Release, Page 1, Paragraphs 1-3) and the advantage of allowing an application to sign transactions on behalf of the user (Lapstun, column 33 lines 53-56).

6. With regards to claims 2, 11, 16, 30, 35, 42, 51 and 56 Asay as modified teaches the integrating of the application with a directory service for providing access to application-specific certificate for the application (RSA Security Press Release, Page 1 Paragraph 2, Asay column 14 lines 34-37, Figure 3).

7. With regards to claims 3, 22, and 43, Asay as modified teaches the directory service comprising one of a LDAP service, an X.500 directory, and a database (Asay column 14 lines 34-37).

8. With regards to claims 4, 12, 17, 23, 31, 44, 52 and 57, Asay as modified teaches the storing of the application-specific certificates in the certificate repository of the directory service (RSA Security Press Release, Page 1 Paragraph 2, Asay column 14 lines 34-37).

9. With regards to claims 5, 13, 24, 32, 36, 45 and 53, Asay as modified teaches the receiving notice of the master certification authority revoking the master certificate of the subscriber (Asay, column 15 lines 57-60) and the revoking of the application-specific certificate of the subscriber corresponding to the revoked master certificate (Asay, column 15 lines 57-67, RSA Security Press Release, Page 1 Paragraph 2).

10. With regards to claims 6,14, 25, 33, 37, 46, and 54 Asay as modified teaches the storing of the revoked application-specific certificate in a certificate revocation list (Asay, column 23 lines 48-50).

11. With regards to claims 7, 15, 18, 20, 26, 34, 38, 40, 47, 55, 58 and 60, Asay as modified teaches the integrating of the application with a registration authority for registering subscribers and revoking subscribers' certificates (Asay, column 10 lines 25-29), in response to a subscriber being registered issuing an application-specific certificate to the subscriber (Asay, column 10 lines 29-36, RSA Security Press Release, Page 2, Paragraphs 3-4), and in response to a subscriber's certificate being revoked

revoking the application-specific certificate of the subscriber (Asay, column 15 lines 57-67, RSA Security Press Release, Page 1 Paragraph 2).

12. With regards to claims 19, 29, 39, 50 and 59, Asay teaches the integrating a plurality of servers with a server-specific certificate authority for issuing server-specific certificates (Asay, column 10 lines 23-50 "reliance server", column 12 lines 23-28), receiving notice of a registration authority registering subscribers (Asay, column 10 lines 29-36), and issuing to the subscriber a server-specific certificate for use by the server (Asay, column 10 lines 45-50). Asay fails to teach the integrating of the certificate authority into an application and the issuing of application-specific certificates. RSA Security teaches the integrating of the certificate authority into an application (RSA Security Press Release, Page 2, Paragraphs 3-4). Lapstun teaches the issuing of application-specific certificates (Lapstun, column 33 lines 53-56, certificate for each application). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize RSA Security's method of integrating PKI functions into an application and Lapstun's certificate method with Asay's reliance server for integrating transactions because it offers the advantage of simplifying and accelerating the development of PKI enabled applications and providing interoperability with all of the leading PKI platforms (RSA Security Press Release, Page 1, Paragraphs 1-3) and the advantage of allowing an application to sign transactions on behalf of the user (Lapstun, column 33 lines 53-56).

13. With regards to claim 21, Asay teaches the integrating of an server with a server-specific certificate authority for issuing server-specific certificates (Asay, column 10 lines

23-50 "reliance server"), receiving notice of a master certification authority issuing a master certificate to a subscriber (Asay, column 12 lines 17-21), issuing to the subscriber a server-specific certificate for use by the server (Asay, column 10 lines 45-50), and a directory service integrated with the server and configured to provide access to server-specific certificates (Asay column 14 lines 34-37). Asay fails to teach the integrating of the certificate authority into an application and the issuing of application-specific certificates. RSA Security teaches the integrating of the certificate authority into an application (RSA Security Press Release, Page 2, Paragraphs 3-4). Lapstun teaches the issuing of application-specific certificates (Lapstun, column 33 lines 53-56, certificate for each application). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize RSA Security's method of integrating PKI functions into an application and Lapstun's certificate method with Asay's reliance server for integrating transactions because it offers the advantage of simplifying and accelerating the development of PKI enabled applications and providing interoperability with all of the leading PKI platforms (RSA Security Press Release, Page 1, Paragraphs 1-3) and the advantage of allowing an application to sign transactions on behalf of the user (Lapstun, column 33 lines 53-56).

14. Claims 8-9, 27-28, and 48-49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Asay et al US Patent No. 5,903,882 , RSA Security's BSAFE Cert-C software as seen in press release "RSA Security Simplifies PKI Application Development," and Lapstun et al US Patent No. 6,549,935, as applied to claim 1 above,

and further in view of Otway US Patent No. 6,192,130. Otway discloses an information security subscriber trust authority transfer system.

15. With regards to claims 8, 27, and 48, Asay as modified fails to disclose the encrypting of the private key of the application-specific certificate with the public key of the master certificate. Otway teaches disclose the encrypting of the private key of the application-specific certificate with the public key of the master certificate (Otway, column 6 lines 31-53). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Otway's method of encrypting private keys with Asay as modified because it offers the advantage of helping ensure than an attacker cannot readily obtain a private key (Otway, column 1 lines 20-34).

16. With regards to claims 9, 28, and 49, Asay as modified teaches the decrypting of the private key associated with the application-specific certificate using the private key associated with the master certificate (Otway, column 8 lines 28-47) and authenticating the subscriber for the application using the decrypted private key (Asay, column 16 lines 21-28, column 1 lines 40-45).

Conclusion

17. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

18. de Silva et al US Patent No. 6,615,347 discloses a digital certificate cross-referencing system.

19. de Silva et al US Patent No. 6,564,320 discloses the local hosting of digital certificate services.

20. RSA Data Security's "Understanding Public Key Infrastructure" white paper teaches a key management system.

21. RSA Security's press release "RSA Security Adds Java PKI Softare to its RSA BSAFE product line" discloses the integration of PKI components with applications.

22. MacTech article "RSA Introduces Keon Software" disclosesa family of enterprise PKI products for enterprise customers and developers.

23. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L. Nalven whose telephone number is 571 272 3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on 571 272 3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Nalven

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100